Smart Insulating Container with Anti-Theft Features by M2M Tracking

Cheng-Ting Lee[*], Chun-Min Chang[*], Chung-Yi Kao[*], Hua-Min Tseng[*], Henpai Hsu[*],
Chin-Chung Nien[†], Li-Huei Chen[†], Li-Yen Lai[†], Troy-Chi Chiu[†], Pai H. Chou[‡*]
[*]Department of Computer Science, National Tsing Hua University, Taiwan
[†]Industrial Technology Research Institute(ITRI) Hsinchu, Taiwan
[‡]Department of Computer Science, University of California, Irvine, USA
sunkist0704@hotmail.com, {chun.m.chang, backman.only, thm822, dreamfliper}@gmail.com,
{CCN, IvyChen, Brucelai, TroyChiu}@itri.org.tw, pai.chou@gmail.com

***Abstract*—This paper describes a smart insulating shipping container with anti-theft features based on M2M communication for mutual tracking. The container includes a wireless sensor node for sensing the temperature and moisture of the interior of the container as well as the vibration and orientation to ensure integrity of the contents. In case of abnormal conditions, the node notifies the deliverer wirelessly on the smartphone. A distinguishing feature of our container is its anti-theft feature. It detects unauthorized opening of the container lid using a magnetic sensor on a satellite node, and it detects unauthorized removal of one or more containers by exploiting the proximity scanning feature in the Bluetooth 4.0 Low Energy Technology (BLE) already used for its data communication. Experimental results show that not only are our anti-theft and shake detection features effective and responsive but also of low overhead.**

I. Introduction

Smart insulating shipping containers are an important technology for ensuring the integrity of shipped goods in logistics. Insulation ensures that the containers maintain the target temperature range with the aid of active or passive cooling or heating elements such as ice packs. What makes these containers smart is their ability to monitor the interior temperature and other conditions of the container during shipping and notifying the deliverer in case of abnormal conditions, so that remedial actions can be taken promptly before the shipped goods spoil.

Although smart insulating containers have been proposed, they may be limited in a number of ways. First, the on-board sensors of today's containers are primarily limited to tracking temperature only, which is important but may be insufficient. They neglect other potentially important aspects, such as excessive shaking or toppling. For goods that must be kept warm rather than kept cold or frozen, it may be necessary to track the moisture level. Second, there is currently no way to detect and notify the user when a thief tries to steal either the goods or the container while the deliverer steps away from the vehicle during the actual delivery. Together, these features are important for logistics companies, because they are liable for delivering the goods in a proper manner, and such extra assurance can turn into opportunities for added-value services [1].

We propose to overcome problems with today's smart containers by adding the missing features while minimizing the added cost. First, we add a moisture sensor in combination with the temperature sensor for moisture sensing, and we add a triaxial accelerometer for detecting both excessive shaking and toppling. Second, for detecting unauthorized opening of the container while the deliverer steps away, we use a magnetic sensor. Third, to detect unauthorized removal of the container from the vehicle, we implement M2M tracking as enabled by the Bluetooth Low Energy (BLE) based module for wireless communication already in use for notifying the deliverer on the smartphone, without extra hardware cost and with minimal energy overhead.

BLE represents one of the fastest-growing wireless technologies for the Internet of Things (IoT). One reason for its popularity is its very long battery life: a slave can last for one year on a CR2032 coin-cell battery while maintaining a logical connection with a master. Second, it is directly compatible with smartmobile devices (smartphones and tablets) without requiring infrastructure or dongles. In the past year, many BLE devices in the form of sports and fitness monitors, proximity tags, toys, and low-power wearable devices have been introduced to the market. Although they may appear unrelated to the smart insulating containers, the communication protocol can turn out to be an important mechanism for tracking lost or stolen containers after they lose contact. Through mutual scanning and cooperative upload of encountered node IDs to the cloud, there is hope for locating lost containers with the help of cooperating BLE devices that come and leave the wireless range of the lost container. This feature can be enabled at no hardware cost and very little power, code, and memory overhead.

The rest of this paper is organized as follows. We first survey related work on smart containers and identify their strengths and weaknesses. We describe the hardware feature of our system, followed by a description of the anti-theft features. We evaluate our system by replaying a real-world application scenario and show that it has the capability to not only detect and notify the user of abnormal theft activities but also can help locate stolen containers after they lose contact, all without extra hardware features.

II. Related Work

A. Smart Shipping Containers

Smart insulating shipping containers have been proposed by previous work on cold-chain logistics. They can maintain temperature by active temperature control such as a vehicular refrigerator [2] or a thermoelectric cooler (TEC). However, running these active cooling mechanisms require power, which must be drawn from its own batteries or the delivery vehicle's 12 VDC [3]. Therefore, they incur fuel overhead directly or indirectly, making them more costly to operate, and therefore their applications are limited to mainly goods that require precise temperature control, such as serum, donated organs, or other medical-grade items. For vehicular logistics, it is more practical to use passive cooling in the form of gel packs, blue ice, or frozen blocks [4]. They can last for up to an entire day without consuming fuel or other power sources, and they can be replaced easily.

Whether active or passive cooling is used, the temperature-maintenance performance is insufficient unless monitored using temperature sensors. Monitoring can be done using a temperature sensor or a thermocouple, but how to notify the vehicle driver is the more interesting problem. The temperature may be displayed on an LCD on the exterior of the container [3], but the deliverer would need to periodically inspect the temperature readings visually to detect temperature alerts manually. A more practical solution is to use a wireless connection such as Bluetooth [2], ZigBee [5], or Bluetooth 4.0 Low Energy (BLE) [4] to notify the deliverer wirelessly. Bluetooth or BLE have the advantages of being directly compatible with smartphones, tablets, or PCs without requiring a dongle or a protocol bridge.

None of the existing temperature-monitoring containers are designed with anti-theft features in mind. The closest is one that transmits its geocoordinate stamps along with temperature data via cellular data (GPRS) back to the logistics center, so that some tracking is possible [5]. However, it does not deter thieves in action. The container cannot detect if the thief opens the lid and removes the content. Should the thief take the container, the geocoordinate log would just show the location where the container last transmitted its data but would not be able to trace it after it is lost. What is needed are alert and deterring mechanisms that alert the deliverer when the thief opens or moves the boxes, and some way of tracking containers after they lose contact.

In terms of sensing capabilities, virtually all previous systems are designed for cold-chain logistics, but they are not applicable to other temperature ranges. For example, delivery of hot food such as fried rice, hot soup, pizza, and other hot-food items is done today using a combination of meal-sized thermo-containers put inside styrofoam bins. These do not monitor temperature, but instead rely on delivery within 30-60 minutes. One issue with delivering goods in the hot-food temperature range is moisture. That is, steam from the food could condense and negatively affect the texture or flavor of the food. Another possible problem is that the moisture could be a result of a leaky or toppled container or a leaky lid. Detection of moisture and alerting the deliverer promptly is therefore important for correcting these problems.

In terms of monitoring other aspects that may be of interest to shipping, Federal Express makes a module named SenseAware [1] that is placed inside a shipping container (not necessarily thermally insulating) with GPS, barometer, thermometer, relative humidity, and light sensors. The light sensor would be used for detecting opening of the container. Their sensing capabilities and the goal of customer assurance are somewhat similar to ours, but the anti-theft approaches are quite different and complementary. Theirs is a separate sensor box that is placed inside the package, rather than being built into the container. Theirs can transmit data wirelessly to be tracked by their customers on the website, but they do not use M2M communication for anti-theft; the only mechanism is the light sensor but without any deterrence.

B. Finding Lost Items by Proximity Sensing

Proximity tagging is one of the fundamental applications of BLE. A proximity tag is a slave that periodically transmits identifying information for the purpose of opening a lock as a *keyfob* or finding lost items as a *sticker* using a smartphone. They approximate the range of the tag by the RSSI (receive signal strength indicator) level. More recently, two-way tags can help finding a lost smartphone by transmitting a command to make an identifying sound on the smartphone. Additionally, newer-generation proximity tags enable any smartphone owner to opt-in to help find other people's lost items by recording and reporting the scan history to a cloud service.

C. Trajectory Tracking

Constandache et al [6] proposes a way of tracking logical trajectories of devices using audio beacons placed at arbitrary locations. Routing between any two devices can be computed dynamically along the logical locations based on the relationships between the devices and the beacons. Although audio works, we believe that Bluetooth 4.0 Low Energy (BLE) can be more effective than audio for at least two reasons. First, BLE is more reliable than audio while consuming less power. Second, BLE-based systems can be more cost effective because they can be implemented as a few KB of firmware to existing BLE devices such as smartphones, activity monitors (e.g., Nike Fuelband), and BLE lightbulbs (e.g., Philips Hue) without additional hardware cost.

[7] shows the feasibility of trajectory tracking by some anchor sensors based on encounter history. With a sufficiently large number of fixed beacons as anchor sensors, the error distance may be reduced to less than 1 meter. [8] presents a technique for trajectory estimation based on both encounter history and geographical information. As more-powerful devices such as smartphones can readily obtain geocoordinate stamps using the OS's location service, this technique also can be incorporated into our work. One can predict the location of a tag from encounter history without geocoordinate stamp in the location in the spatio-temporal context [9], [10] and by interpolation [11].

We propose to generalize these ideas to the antitheft detection and tracking for our smart containers. Specifically, we extend the M2M communication technique with mutual tracking. The more data that the cloud server collects, the more precisely that the trajectories or locations can be estimated.

III. TECHNICAL APPROACH

We propose to build in the required sensors into the smart container, and we exploit proximity tag features of BLE for anti-theft features. The temperature and moisture sensing parts are well understood, so we will focus the discussion primarily

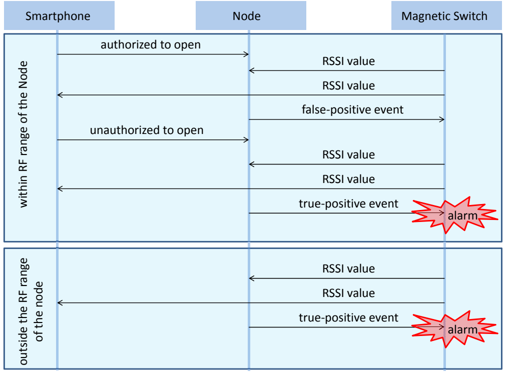


Fig. 1: Opening Detection Flow

on the aspects related to the anti-theft features. The container should be able to detect theft and respond if possible; if not, then it should track the trajectory of the container. Theft can happen when the deliverer temporarily steps away from the vehicle to make the actual delivery. Theft can be either unauthorized removal of content from the container and of the container itself. Our problem statement can therefore be divided into detection, deterrence, and tracking. Our approach to these problems are M2M communication. Our assumption is that our smart container uses BLE transceivers that act as slaves that pair with the deliverer's smartphone.

A. *Unauthorized Opening Detection*

The first type of theft is unauthorized opening of the container's lid when the deliverer steps away. To detect opening of a lid, we can use a magnetic sensor. The lid contains a magnet, while the container's top rim that contacts the lid contains a magnetic switch. When the lid is closed, the magnet is right next to the switch, and its magnetic field disengages the switch. When the lid opens, the magnet moves away from the magnetic switch, and the removal of the magnetic field causes the switch to close so that the node now can have a chance to notify the user of a lid-opening event.

Note that not all lid-opening events are theft events: the deliverer and perhaps the packer are authorized to open and move contents into and out of the container, and such false-positive events should be suppressed. It is relatively easy to detect by M2M proximity sensing: either the node or the smartphone can detect each other's RSSI value, which drops by $1/R^2$. This means it is easy for the user's smartphone to detect if the magnetic-switch node is within reach or out of reach.

On the other hand, when it detects a true-positive event, the deliverer may be outside the RF range of the node such that notification will fail. However, just because the node is out of range of the smartphone does not automatically imply there is a theft event. However, it is easy for the node to decide: if the the deliverer's smartphone is out of range when the lid is opened, then the only thing the node can do is deterrence by sounding an alarm by itself. Fig. 1 shows the flow of our detection of unauthorized lid-opening events.

B. *Unauthorized Removal of Container*

If instead of removing the content, which would trigger an alarm, the thief could remove unsecured containers without triggering the alarm. For a container to detect that it has been stolen, we can also apply M2M proximity sensing, depending on the type of logistics arrangements. One way is to detect if a container has been lifted when the authorized person is not in proximity, similar to the use of proximity sensing to detect unauthorized opening. Lifting can be detected by the accelerometer in terms of a recognizable acceleration pattern, which is sufficiently distinct from the ambient vibrations such as that caused by the idle engine of the delivery truck. In case the notification fails, the main node can also trigger an alarm for deterrence, just as in the case of unauthorized opening (Section III-A).

Another way to detect unauthorized removal of a container is to use M2M communication. This is applicable to the case where the delivery truck carries multiple smart containers, and that these nodes perform their usual proximity sensing with each other and can also be told by the master what other nodes travel with the group. Depending on the placement and stacking of the containers, a node might not be able to detect all other nodes in the group at all times, but that would not be necessary; as long as each node can detect the set of nodes in its proximity then it can assume that it is still traveling with the rest of the group. However, if the set of its neighbors suddenly changes — specifically drops in RSSI sharply and it fails to find any of its group members and the master — then it can conclude that a theft event of the container has occurred. In this case, the stolen container could try deterrence by triggering the alarm, although the effectiveness may be limited. The other containers may also detect that one or more of their peers have disappeared. They should attempt to confirm with each other that none of the nodes in contact can find the missing peer(s). Once confirmed, they can conclude that the theft event has indeed occurred, and one of the nodes should attempt to notify the deliverer on the smartphone.

A special case is a delivery motorcycle with a single container without peers. To solve this problem, we put a vehicular unit as a stand-in for its peer. It is essentially the same node as that on the container but without the sensors, and the detection algorithm can be the same.

C. *Tracking of Lost Containers*

Despite all the anti-theft and deterrence mechanisms, a container can still be stolen by a quick thief while no bystanders are around. Instead of taking no action, we want our stolen container to be able to leave digital "bread crumbs" whenever possible so that it has the chance of being found. The idea is that even though the container cannot contact its owner directly, it will likely encounter other passersby devices that participate in cooperatively finding lost items. Then, it is through other people's devices that the stolen container has a chance of dialing home.

The digital bread crumbs left by the container can be implemented, not surprisingly, by proximity sensing in BLE. That is, the container acts as a proximity tag that scans other tags within its RF range and records the IDs of all tags that it encounters, along with the timestamps. We assume that given

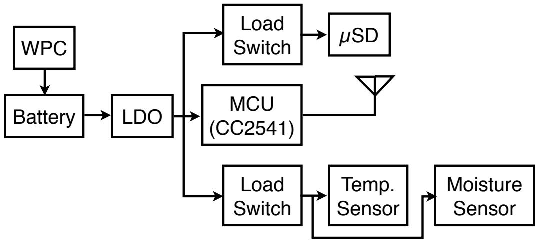


Fig. 2: Block Diagram

the growing popularity of these tags, the container will likely encounter at least some participating smartphones and tags, even if they are in vehicles in the next lane on the road or sidewalks.

We assume that the more powerful devices such as smartphones can log additional information such as geocoordinate stamps in addition to the temperature, moisture, and acceleration data. Other devices such as fixed light switches or iBeacon-compatible devices would have fixed, known locations that can be recorded in a database, so that the location can be inferred by the RSSI. A smartphone that participates in lost-item tracking would periodically upload the log to a cloud service that anonymizes its users for privacy protection, but can selectively make intersecting data available. In addition, any other BLE tags can also log encounters with the stolen container as a proximity tag, and any of them can upload their encounter history to the server via their owner's smartphone, with or without geocoordinate stamps. The position can be estimated using either historical data or using the space-time intersection of the lost container (as a tag) with other devices and construct a *trajectory* from their encounters over time [9]–[11]. In the worst case, there is no geocoordinate information from the encounter history collected by the server, but the logical encountering history of the owners can still be identified [6]. In any case, given the general trends, investigators would have a better chance of focusing in on where the lost container may have been to give them more clues on how to recover it.

IV. Hardware

This section describes the hardware of our proposed smart insulating container. The hardware has a similar architecture to the EcoBT node [12] as used in the IISC [4] in that it is centered around an integrated microcontroller unit (MCU) with the integrated BLE transceiver and protocol stack, although we choose a more energy-efficient MCU. We have a much richer collection of sensors and mechanisms for saving power during idle time. Moreover, our hardware includes an entirely separate satellite board that implements the magnetic sensor with its own BLE MCU. This structure simplifies the container design and the manufacturing process. The next two subsections describe the main sensor node and the satellite node.

A. Main Sensor Node

The main sensor node is organized into five subsystems: the controller, sensors, data storage, real-time clock (RTC), and power.

1) Controller Subsystem: The controller subsystem consists of the TI CC2541 MCU with integrated BLE transceiver. It contains an 8051-compatible MCU core with 8 KB SRAM and 256 KB code flash. It is used as both the controller to all sensing devices and the communication module to the deliverer's smartphone. The firmware is compiled and linked with the BLE stack provided by TI. It is driven by a 32 KHz crystal to enable waking up from mode 2, i.e., upon receiving an RF packet.

2) Sensor Subsystem: The sensor subsystem consists of a thermocouple, a moisture sensor, and a digital triaxial accelerometer. The thermocouple and moisture sensor are bundled together as one unit inside a metal tube that is inserted through a hole to the interior wall of the container while enabling the rest of the electronics to remain on the outside for simpler service and wireless transmission. The electrical signals from these two sensors are digitized by an integrated circuit designed specifically for the combination of thermocouple and moisture sensor. This allows the additional function without occupying additional area.

The triaxial digital accelerometer is soldered directly on the same circuit board as the MCU. It transfer data over SPI and includes two interrupt outputs, one for the high threshold and one for the low threshold. The threshold values for the three axes are programmable, and they can be composed conjunctively or disjunctively for the purpose of threshold testing. The accelerometer serves two purposes: as both a vibration sensor and as a tilt sensor. That is, fluctuations in the acceleration data are a direct indication of the forces experienced by the container and its content. At the same time, the earth exerts 1 g gravity in the $-Z$ direction. After removing fluctuations, the DC component can be interpreted as a reasonable estimate for the orientation. After adding in the trends and the impact upon hitting ground, it is possible to detect the signature of a box toppling.

3) Data Storage Subsystem: The main sensor node contains an expansion slot for data logging onto a micro Secure Digital (MicroSD) flash memory card. It is an option in case the user wants to maintain an event log.

4) Real-Time Clock Subsystem: The real-time clock subsystem is implemented using an RTC chip over I^2C. It tracks not only the hour, minute, and second but also the day of the week, day, month, year, and century. It also allows the user to set a time for the alarm. It can be used for supporting power management by providing a wake-up interrupt signal. The RTC subsystem can either be powered by the same battery or its own dedicated coin-cell battery.

5) Power Subsystem: The power subsystem includes the battery, voltage regulator, inductive charger, and load switches. We use a 700 mAh lithium-polymer battery for high energy density. The battery can be charged by USB or inductively using the Qi standard. The Qi power receiver module includes the receiving coil and the charger board for the lithium-polymer battery. The output of the battery is connected to a DC-DC converter with low quiescent current. Even though the MCU contains an on-chip LDO, its range is lower than the minimum voltage of the lithium-polymer battery and therefore the voltage must be stepped down first. Besides, other sensor modules require also lower voltage than the battery but they do not contain built-in regulators. Some sensor modules continue to consume power even though they are not active and do not support power management. To conserve power for those devices, we added a load switch that disconnects supply power to them.

B. Satellite Node with Magnetic Switch

The satellite node is a specialized node with a BLE MCU and a magnetic sensor. The BLE MCU is the μEnergy integrated MCU, CSR1010, which contains 64 KB RAM and 64 KB ROM. We use it instead of the TI CC2541 for lower cost (US$1.065 @2ku), smaller footprint (5 mm× 5 mm) and lower power consumption. It interfaces with the magnetic switch tied to its interrupt input line. When a magnetic field is applied near the magnetic switch, it "disconnects" the switch to generate a shut-down signal. When the magnetic field is removed, the switch closes and outputs a high value that enables the node to boot up quickly and run. In other words, the magnetic switch effectively wakes up the CSR chip so it can attempt to either pair with the master or send a broadcast message without pairing as part of announcing that the lid on the container has been opened. Just opening the lid does not imply an alarm; instead, it depends on the context of the deliverer.

V. Software

Software for the smart insulating container is divided into the firmware for the nodes, app software on the smartphone, and software on the backend server. The firmware is further divided between the main node and the satellite node, and the two communicate wirelessly with the smartphone that acts as the uplink to the backend server.

A. Firmware

The firmware on the main node follows the general structure for the CC2541 MCU. The most important part is the BLE protocol stack, which requires TI's OS Abstraction Layer (OSAL). OSAL is an OS-like software layer that supports task dispatching and basic services such as memory management, and it is required for using the BLE stack. The user writes C code for the profiles and application to be compiled and linked with the stack and system software to form the firmware image. In BLE, a *profile* is defined in terms of a set of *characteristics values* and *descriptors* for a collection of services, such as human-interface devices (HID), blood pressure monitors, proximity tagging, etc. In addition, all BLE devices implement the Generic Attribute Profile (GATT) to enable devices to discover each other's capabilities dynamically. Profiles essentially standardize the message formats for M2M interactions so that they can work out-of-the-box without additional driver installation.

Our firmware implements a smart-container sensing data profile and the proximity sensing profile. The former is a custom profile that enables the different sensing data to be queried and a number of attributes (e.g., sampling rate, data download, etc) to be read and written. The proximity profile enables the container's main node to also act as a proximity tag. It can pair with the deliverer's smartphone and periodically scan and track each other's proximity.

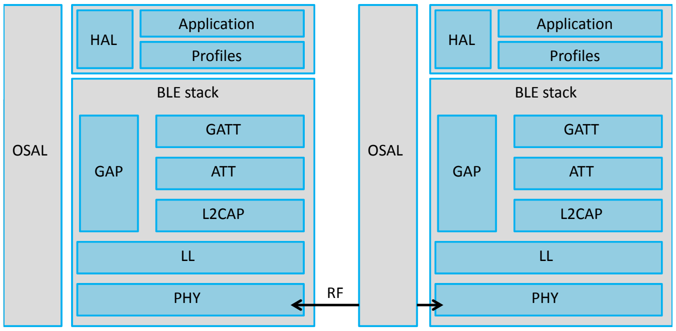


Fig. 3: Software Stack

B. Smartphone App

We have written an app for iOS 7 with ongoing work to port it over to Android. iOS includes support for the BLE protocol stack. The app enables the user to pair the smartphone (iPhone 4S or later) as BLE master with one or more nodes in the smart containers as slaves. The iPhone can send commands to the containers using the profile we define for the container application. The commands can include setting the RTC, setting the update interval, RF and acceleration threshold values, and other preferences. In addition to responding to commands, the container's node can also actively push alert events by the *notification* mechanism in BLE. For example, in the case the container topples, the accelerometer's threshold detector pushes the event to the smartphone app, which then renders the sound and vibration to alert the deliverer.

C. Backend Server

We use an existing backend server already in use for cold-chain logistics but augment it with the proximity tag support. It is a service-oriented architecture (SOA) that can be configured to provide a wide range of performance, flexibility, and scalability requirements. The JBoss SOA-P middleware integrates modules that provide JavaEE5-compliant web services that can exchange data, and JBoss ON enables cloud-like availability by load balancing. Data is stored in MySQL for not only logged data and inventory control but also asset management. This custom backend has been in use for an existing cold-chain logistics with minimal extensions for the additional sensor data fields.

The more important extension is the backend for supporting proximity tag tracking. Participating smartphones can upload their scan history of proximity tag IDs with time and location stamping to the backend server. Other participating tags can also transmit their scan history of the IDs and time stamps, even without location stamps, and the backend server will use the space-time intersection to construct the trajectory of each tag by best effort. The backend server is organized to be expandable such that additional sensing fields such as altitude, acceleration, compass, and other types of data can all be incorporated to further help refine the trajectory of the tag being tracked.

VI. Evaluation

We have a prototype of our smart insulating container with an implementation of the anti-theft features. This section

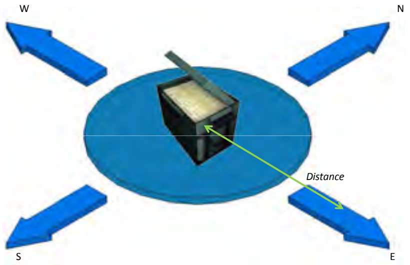


Fig. 4: Direction of Magnetic Switch

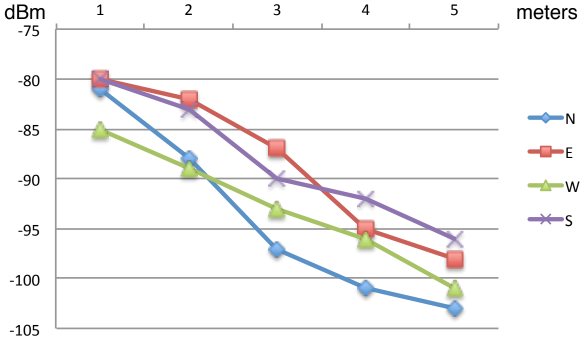


Fig. 5: RSSI value over distance.

presents evaluation results that show the effectiveness of our technical approach. We also evaluate the boot-up time of the satellite node for the latency.

A. *Unauthorized Opening*

Unauthorized opening is defined to be the conjunction of an opening event and the absence of the authorizing tag in proximity. We therefore test the sensitivity of the magnetic switch and the proximity sensing together.

1) Sensitivity of Magnetic Switch: The selected magnetic switch should be sensitive to the chosen magnet in its installed configuration. When the magnetic switch experiences a magnetic field greater than 15 Gauss, it opens (disconnects), and this is easily achieved by a conventional magnet, which has a magnetic field much greater than 15 Gauss relative to the magnetic switch when the lid is closed. When the sensed magnetic field drops below 12 Gauss, then the magnetic switch closes (connects). In our tests, when the distance is about 3∼5 cm when the switch closes.

2) Proximity Sensing for Authorizing Tag: We tested the RSSI value of the tag as measured by a smartphone over different distances and directions. Fig. 4 shows the different directions with respect to the container itself, while Fig. 5 shows the RSSI value in dBm over distances from 1 to 5 meters. As the measurement result shows, the RSSI is a reasonably good indicator for the trends in the relative distances in all four directions.

3) Boot-up Latency of Satellite Node: We also evaluate how quickly the satellite node can wake (or boot) up when triggered by the magnetic switch. The latency is important because the satellite node must be able to boot up fast enough or else it risks being yanked by the thief. According to our measurement results, the booting time of the satellite node from powering on to completing the booting process takes 0.4 sec, which is sufficiently fast to notify the user before the thief has a chance to defeat this anti-theft mechanism.

B. *Unauthorized Moving of Container*

Fig. 6 show the container in different orientations and the corresponding acceleration time-history plots, while Fig. 7 shows the photos of the respective configurations. The static orientation of the container can be determined by the measured acceleration of the gravity vector in the absence of linear acceleration.

From the acceleration, we can distinguish among lifting, moving, and toppling from the static configurations primarily by the sudden acceleration upon impact.

C. *Discussion*

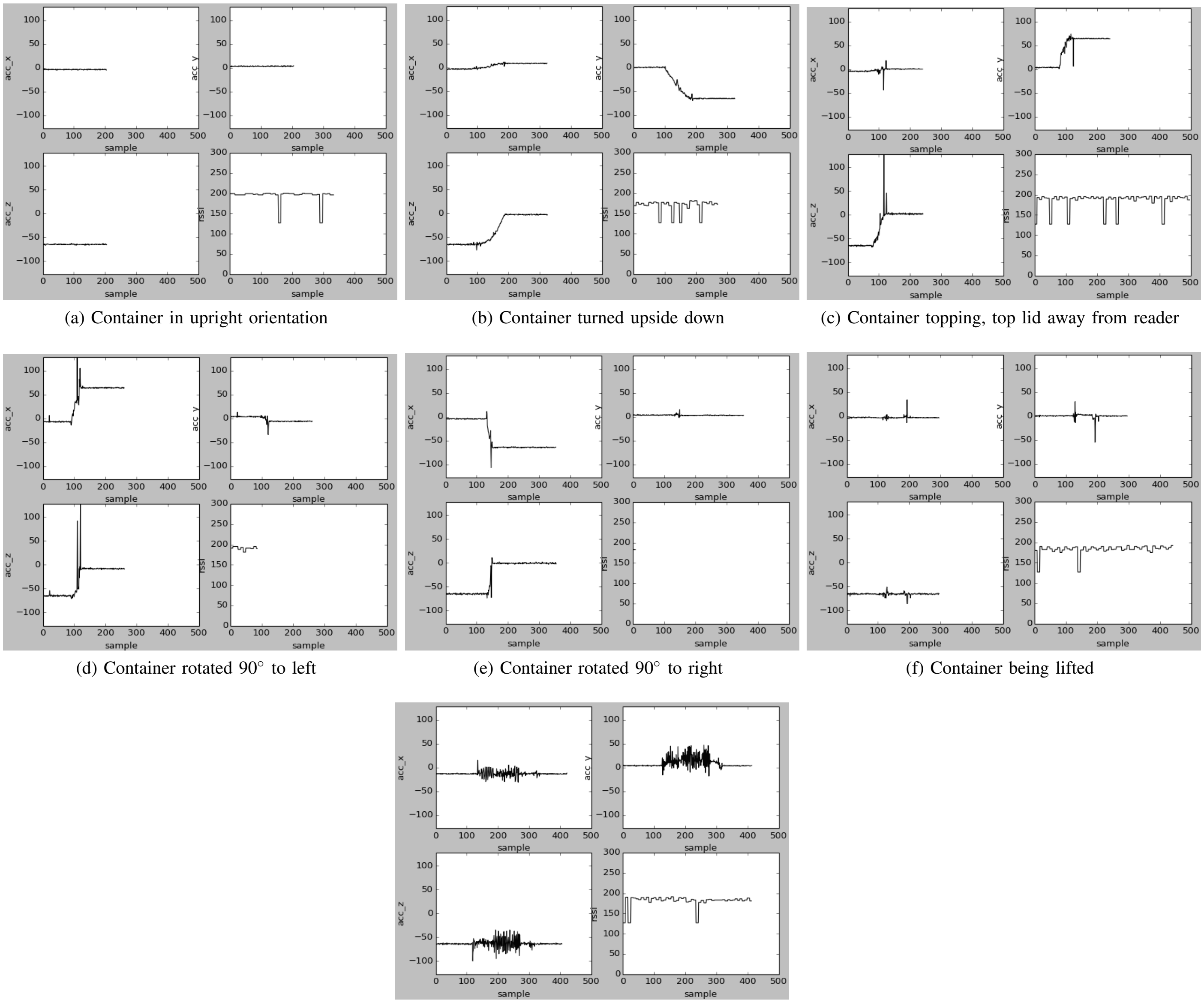
Our technique is not foolproof and can still be defeated by a skillful thief. For instance, to foil the opening detection, a skilled thief could use a very strong magnetic positioned precisely to keep the magnetic switch engaged. A skillful thief would be able to prevent detection of acceleration-based unauthorized lifting by moving the container with slowly minimal acceleration. Alternatively, a thief can simply inject RF interference as well as audio noise injection to overwhelm the alarm. To make lid-opening detection more robust, we could add a light sensor as SenseAware has done, but that can also be easily defeated by opening in the dark; or we could add a rotation sensor (e.g., a rotation-style potentiometer) to the hinge of the container. However, our container uses no hinges, as it would complicate the physical design. For now, we believe the magnetic sensor represents a good balance between effectiveness and ease of manufacturing.

In the case of a delivery truck, the container is shipped with a group of other containers, which we also assume to be smart and BLE-enabled. We further assume that the thief cannot remove the entire group of boxes at a time, but that each box is moved individually. Our system can be effective at detecting these representative theft events, but we cannot guarantee that they can cover all cases.

The use of M2M features in BLE may not be so effective today as the tags are only beginning to appear on the market; but if some day these tags become ubiquitous, their chance of being able to leave digital bread crumbs and dial home will be excellent after they lose connection with the deliverer's smartphone or the hub in the vehicle. Before that happens, an interim solution would be to add a cellular data module, such as a GPRS modem, which can be inexpensive and effective at dialing back. However, such a unit must be carefully power managed or else it can exhaust the battery energy too soon.

VII. Conclusions

We have presented a new design of a smart insulating shipping container that not only monitors the shipping conditions but also several novel anti-theft features. It uses a combination of M2M communication and sensors. Specifically, we use a magnetic sensor to detect lid-opening events that



(a) Container in upright orientation

(b) Container turned upside down

(c) Container topping, top lid away from reader

(d) Container rotated 90° to left

(e) Container rotated 90° to right

(f) Container being lifted

(g) Container being moved while lifted

Fig. 6: X, Y, Z acceleration time histories and RSSI values of the container in different conditions.

imply content removal, and we use an accelerometer to detect container removal. The proximity sensing feature enabled by BLE protocol provides the context necessary to determine if the event is unauthorized and triggers an alarm or notification accordingly. We further exploit M2M communication to detect if one or more containers have been detached from their peers.

Acknowledgments

This work is sponsored in part by the Ministry of Economic Affairs through the Industrial Technology Research Institute (ITRI) subcontracts SSTC-102-65-02 and SSTC-103-65-02.

REFERENCES

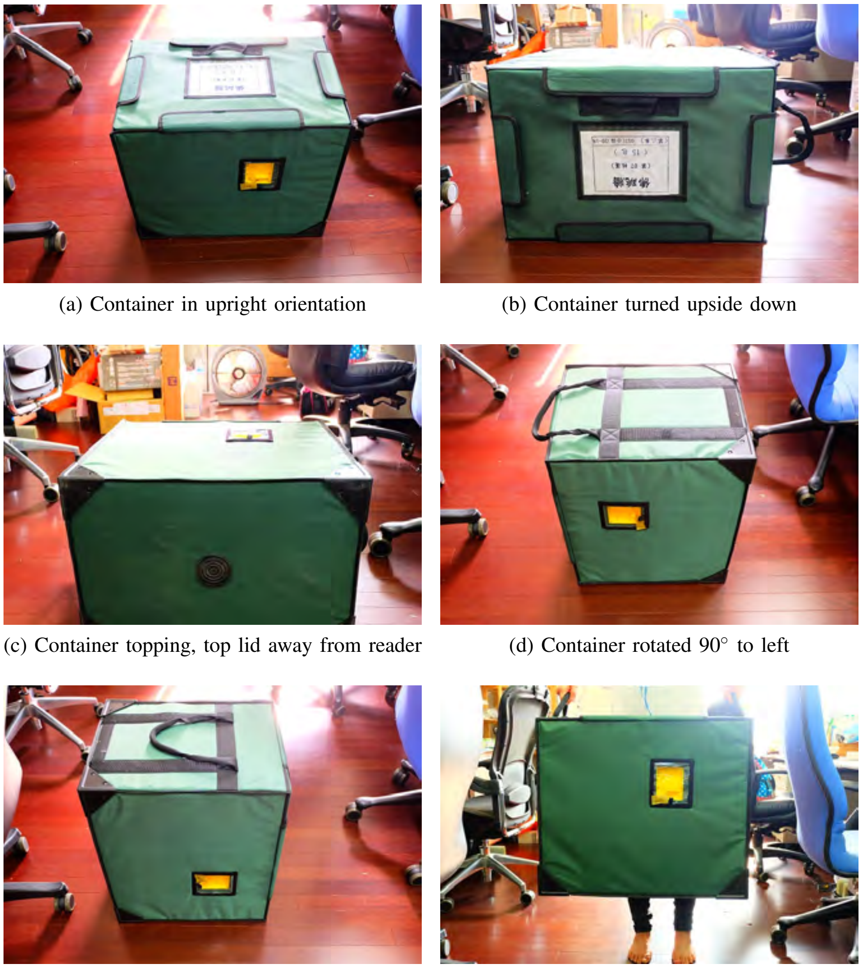
[1] FedEx, "SenseAware^{SM} – a shipment tracking and monitoring service powered by FedEx," http://www.senseaware.com, 2014.

[2] Q. Shan and D. Brown, "Wireless temperature sensor using Bluetooth," *Proc. IWWAN, London, UK*, 2005. [Online]. Available: http://www.ctr.kcl.ac.uk/IWWAN2005/papers/22.pdf

[3] AcuTemp, "Cold chain shipping containers, temperature sensitive insulated boxes, thermal management solutions," http://www.acutemp.com, 2013.

[4] P. H. Chou, C.-T. Lee, Z.-Y. Peng, J.-P. Li, T. K. Lai, C.-M. Chang, C.-H. Yang, Y.-L. Chen, C.-C. Nien, L.-H. Chen, L.-Y. Lai, J.-C. Lu, and S.-C. Hung, "A Bluetooth-Smart insulating container for cold-chain logistics," in *Proceedings of the 2013 6th IEEE International Conference on Service Oriented Computing and Applications (SOCA)*, Kauai, Hawaii, USA, December 2013.

[5] Y. URSA, P. Perez, and A. Meissner, "Cold-Trace: a mobile-based traceability solution rendering fleet management more effective," in *Exploiting the Knowledge Economy: Issues, Applications, Case Studies*, P. Cunningham and M. Cunningham, Eds. Barcelona, Spain: IOS Press, 2006.



(a) Container in upright orientation

(b) Container turned upside down

(c) Container topping, top lid away from reader

(d) Container rotated 90° to left

(e) Container rotated 90° to right

(f) Container being lifted, and then moved

Fig. 7: Container orientation for the configurations in Fig. 6.

[6] I. Constandache, X. Bao, M. Azizyan, and R. R. Choudhury, "Did you see Bob?: human localization using mobile phones," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 2010, pp. 149–160.

[7] A. Symington and N. Trigoni, "Encounter based sensor tracking," in *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2012, pp. 15–24.

[8] S. Fujii, A. Uchiyama, T. Umedu, H. Yamaguchi, and T. Higashino, "Trajectory estimation algorithm for mobile nodes using encounter information and geographical information," *Pervasive and Mobile Computing*, vol. 8, no. 2, pp. 249–270, 2012.

[9] H. Gao, J. Tang, and H. Liu, "Mobile location prediction in spatio-temporal context," in *Nokia Mobile Data Challenge Workshop*, Newcastle, UK, June 18-19 2012. [Online]. Available: https://research.nokia.com/files/public/mdc-final72-gao.pdf

[10] G. Yavaş, D. Katsaros, Ö. Ulusoy, and Y. Manolopoulos, "A data mining approach for location prediction in mobile environments," *Data & Knowledge Engineering*, vol. 54, no. 2, pp. 121–146, 2005.

[11] B. Yu and S. H. Kim, "Interpolating and using most likely trajectories in moving-objects databases." Springer, 2006, pp. 718–727. [Online]. Available: http://csit.udc.edu/~byu/DEXA06preprint.pdf

[12] A. Wang, Y.-T. Huang, C.-T. Lee, H.-P. Hsu, and P. H. Chou, "EcoBT: Miniature, versatile mote platform based on Bluetooth Low Energy Technology," in *Proceedings of the IEEE International Conference on Green Computing and Communications*, Taipei, Taiwan, September 1-3 2014.